LANCOM Release Notes
Advanced VPN Client macOS 4.61 Rel

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom-systems.com

January 03rd, 2022, CBuersch

Table of Contents

1. Preface

The LANCOM Advanced VPN Client Windows provides mobile employees with encrypted access to the company network, whether they are at their home office, on the road, or even abroad.

This document describes the innovations within the Advanced VPN Client macOS software releases 4.61 Rel, as well as the improvements since the previous version.

2. New features, changes, and history

Advanced VPN Client macOS improvements in version 4.61 Rel Build 29053

Prerequisites

Apple macOS Operating Systems

The following macOS operating systems are supported with this version on hardware with Apple M1 chip or Intel CPU:

- macOS 11 Big Sur
- macOS 12 Monterey

Limitation in version 4.61 Rel

This version of the client, unlike previous client versions, does not include firewall functionality. Users who want to use this firewall functionality should - if possible - use the previous version 4.0 of the client.

Bugfixes / improvements

- **Split tunneling**
  All split tunneling entries are now executed correctly by the client again.
- **IKEv1 rekeying**
  The compatibility of the client with regard to rekeying for IKEv1 with third-party gateways has been improved.

Known limitations

Location for certificate files

Accompanied by modifications for macOS Catalina, the client's p12 certificate files can not be used from random storage locations. In case of the automatically created folders in the user's home directory (e.g. documents, desktop, downloads, etc.) the error message „Access denied" shows up. If certificate files are stored directly to a directory within the user's home directory, accessing the files works.

Advanced VPN Client macOS improvements in version 4.60 Rel Build 29048

Prerequisites

Apple macOS Operating Systems

The following macOS operating systems are supported with this version on hardware with Apple M1 chip or Intel CPU:

- macOS 11 Big Sur
- macOS 12 Monterey

Limitation in version 4.60 Rel

This version of the client, unlike previous client versions, does not include firewall functionality. Users who want to use this firewall functionality should - if possible - use the previous version 4.0 of the client.

New features

- **Support of macOS 11 Big Sur, macOS 12 Monterey as well as the Apple M1 chip**
  The client is compatible with the Apple M1 chip from this version on. The operating system macOS 11 Big Sur or macOS 12 Monterey is required.

Bugfixes / improvements

- **Support for 250 split tunnel networks**
  Up to 250 split tunnel networks are now supported for IPv4 and IPv6 when importing an INI configuration file.
- **DNS domain support in the INI file**
  DNS-Domains, die durch den VPN-Tunnel aufgelöst werden sollen, können nun auch per INI-Datei importiert werden.
- **MFA dialog was not displayed completely**
  Display errors occurred when using multi-factor authentication. The previous display window was too small for particularly long texts.
- **Incorrect caching of domain names when changing profile**
  Domain names were incorrectly cached after profile change.
- **Configuration Split Tunneling: ‚Also forward local networks in the tunnel' added**
  Previously, it was only possible to forward local networks in the tunnel in the Windows client. This is now also possible in the macOS client.
- **Unintentional proposal change (DH group) after profile editing**
  If in the INI configuration file the DH group was configured exclusively in the IKEPOLICY section, this value was set to the default value of the DH group after editing the profile in the client.
- **Configuration change from IPv4 to IPv6**
  After switching in the profile from IPv4 to IPv6, the IPv6 table was not available under Split Tunneling.

- **Support for PEM and DER format regardless of file extension**
  Previously, only files with .pem file extension were read as PEM format, all others were read in binary DER format only. Now DER and PEM format are also supported for .cer and .crt file extensions.
- **Missing menu bar after starting the computer**
  After starting the computer, under certain circumstances the client menu bar was not displayed in the foreground despite the client GUI being active.
- **Error importing the configuration locks**
  Importing configuration locks via INI configuration file was incorrect.
- **Update to OpenSSL version 1.0.2u-8**
  The OpenSSL version used in the NCP Secure Client was raised to 1.0.2u-8. This closed the OpenSSL vulnerability CVE-2020-1971.
- **Optimized handling of DNS requests**
  Along with the newly implemented network adapter, the handling of DNS requests has been improved.
- **Improvements in VPN Path Finder in conjunction with a configured proxy**
  If a VPN connection was established using Pathfinder and a proxy for Pathfinder, no request was made to the proxy server. This is now possible due to an improvement in the dynamic configuration transfer.
- **Missing help text**
  In the LANCOM Advanced VPN Client the help text for the function ‚IPsec over HTTPS Proxy' was not displayed.
- **The user rights for the installation directory have been adjusted.**
- **Crash of the ncprwsmac service**
  In rare cases, the ncprwsmac service crashed.

Known limitations

Location for certificate files

Accompanied by modifications for macOS Catalina, the client's p12 certificate files can not be used from random storage locations. In case of the automatically created folders in the user's home directory (e.g. documents, desktop, downloads, etc.) the error message „Access denied" shows up. If certificate files are stored directly to a directory within the user's home directory, accessing the files works.

Advanced VPN Client macOS improvements in version 4.00 Rel Build 46079

Prerequisites

Apple macOS operating systems

The following Apple macOS operating systems are supported by this version:

- macOS Catalina 10.15
- macOS Mojave 10.14
- macOS High Sierra 10.13

New features

- **Full support for macOS Catalina 10.15**

  As from this version, the client is fully compatible to macOS Catalina 10.15.

  During the installation the kernel extension which should be installed has to be allowed explicitly within the security settings.

- **Virtual network adapter**

  The client now obtains its own network adapter. This makes it possible for e.g. VoIP applications to communicate through the VPN tunnel. Furthermore, due to this network adapter, the client can use an IP protocol within the VPN tunnel which is actually not used in the physical network. Example: usage of IPv6 within the VPN tunnel, although only IPv4 is available for the connected network.

- **Connect/Disconnect menu in the dock icon**

  If the VPN client has a configurable VPN profile, the selected connection can be established/disconnected by right-clicking the dock menu icon.

Bugfixes / improvements

- **Optimized handling of DNS requests**

  Associated with the currently implemented network adapter the handling of DNS requests can be improved. Two cases have to be distinguished:

  1. No split tunneling operation

  In this operation mode any communication to other IP addresses which are not located within the currently used IP address range is done through the VPN tunnel. This also covers DNS requests.

  2. Split tunneling operation

  In this operation mode IP remote networks are defined within the split tunneling configuration. If now targets are addressed within the remote network, data is running through the VPN tunnel. All remaining data, particularly DNS requests, is running past the VPN tunnel. Due to this, targets in the remote network can initially not be accessed via their domain names, because generally accessible DNS servers do not typically resolve company-internal DNS names.

  This problem can be solved by the explicit configuration of the internal domain names which are located within

the remote network.

So the entry ‘company.local’ causes the respective DNS requests, e.g. ‘intranet.company.local’ to be sent to company-internal DNS servers through the VPN tunnel.

By this configuration option data traffic through the VPN tunnel or past the VPN tunnel can be separated completely.

- **New connection mode**

  The connection mode “automatic” has been replaced by the mode “always”. If “always” is configured, the client tries to establish a VPN tunnel all the time. This happens, as distinct from the mode “automatic” without queued data which has to be sent.

Known limitations

Location for certificate files

Accompanied by modifications for macOS Catalina, the client’s p12 certificate files can not be used from random storage locations. In case of the automatically created folders in the user’s home directory (e.g. documents, desktop, downloads, etc.) the error message „Access denied“ shows up. If certificate files are stored directly to a directory within the user’s home directory, accessing the files works.

Advanced VPN Client macOS improvements in version 3.20 Rel Build 43098

Prerequisites

Apple macOS operating systems

The following Apple macOS operating systems are supported by this version:

- macOS Mojave 10.14
- macOS High Sierra 10.13
- macOS Sierra 10.12

As from this version, support for OS X Yosemite 10.10 and OS X El Capitan 10.11 expires.

New features

- **IPv6 support**

  The client now supports dual stack operation. Therefore, IPv4 only, IPv6 only or both can be selected in the configuration. Furthermore, split tunneling for both protocols can be configured individually.

- **Dark mode support**

  The client GUI supports now dark mode as introduced with macOS Mojave.

- **macOS keychain support**

  A user certificate can be configured within the computer certificate configuration for usage in macOS keychain. This requires the previous certificate import to the system keychain. Access has to be granted to the enclosed private key by the NCP service ncprwsmac in the folder "/Library/Application Support/NCP/Secure Client/".

Bugfixes / improvements

- **Adaption of the deinstallation routine in macOS Mojave**

  User permission was requested as appropriate on deinstallation for access to the address book, calendar, and photos. Although the deinstallation routine never accessed the mentioned data, this behavior has been fixed now. Likewise, the application icon is now removed correctly from the dock after deinstallation.

Advanced VPN Client macOS improvements in version 3.10 Rel Build 40218

New features

- **Biometric authentication (fingerprint recognition) before VPN connection establishment**

  For protection against a VPN connection establishment by unauthorized third parties a biometric authentication has been added to the Advanced VPN Client. Immediately after pressing the "Connect" button in the client GUI there is a prompt for user authentication. The VPN connection is only established after a positive authentication. Required for biometric authentication is macOS Sierra 10.12.1 or later. If this option is enabled but no Apple hardware with integrated fingerprint sensor is used, the user password is required instead.

Bugfixes / improvements

- **OTP functionality**

  The dialogue box for entering the OTP pass code was not displayed. This bug has been fixed.

- **Certificate fingerprint**

  The fingerprint of a certificate was not displayed within the certificate view. A comparison of the fingerprint for certificate checking could not happen. This bug has been fixed.

Known issues

- Under OS X Yosemite 10.10 the FIPS mode cannot be activated.

Advanced VPN Client macOS improvements in version 3.00 RU1 Build 38902

Bugfixes / improvements

- **Optimized start of system services**

A bigger amount of installed network adapters could cause a failure when trying to start the VPN client.

Advanced VPN Client macOS improvements in version 3.00 Rel Build 37856

New features

- **Support for macOS High Sierra 10.13**
  The Apple operating system macOS High Sierra 10.13 is now fully supported.
- **Support for IKEv2 and IKEv2 Redirect**
  As from this version, the client supports IKEv2 and IKEv2 Redirect. Using IKEv2 Redirect, it is now possible to forward the Advanced VPN Client to another gateway. Ideal for efficient load balancing in environments where multiple gateways are deployed.
- **Support for FIPS mode**
  The client can be installed with Federal Information Processing Standard (FIPS) conformity using the installation routine. FIPS is the term used to describe publicly disclosed United States security standards that are required to be enforced if the client is used in the U.S. With activated FIPS mode all connections are established with algorithms obeying the FIPS standard.
- Modernized graphical user interface of the client

Bugfixes / improvements

- **Improved DPD functionality**
  The Dead-Peer-Detection for VPN connection monitoring has been generally improved.

Advanced VPN Client macOS improvements in version 2.05 RU1 Build 32167

New features

- Support for macOS Sierra 10.12

Known issues

- An online activation is not possible if the 30-day test period has been exceeded. The activation has to be done offline in that case.
  (see: https://www.lancom-systems.com/service-support/registrations/software/activation/)

Advanced VPN Client macOS improvements in version 2.05 Rel Build 23310

New features

- Compatibility improvements for OS X Yosemite 10.10

Bugfixes / improvements

- The NCP service is also started again at system startup.

Advanced VPN Client macOS improvements in version 2.05 Rel Build 14711

New features

- Support for OS X Mavericks (10.9) (minimum requiremets OS X Mountain Lion 10.8)

Bugfixes / improvements

- If the smartcard is removed during operation, an existing VPN tunnel is not disconnected.

Advanced VPN Client macOS improvements in version 2.02 Rel Build 0014

New features

- DNS requests for a domain can be resolved through a VPN tunnel independent from split tunneling.

Bugfixes / improvements

- Improved profile selection on the client user interface
- When using external xAUTH authentication the dialogues for central site password query are displayed correctly.

Advanced VPN Client macOS improvements in version 2.02 Rel Build 0011

Bugfixes / improvements

- The LANCOM Advanced VPN Client can be used under OS X Lion 10.7.
- Path extension to 250 characters for the PKCS#11 module

Advanced VPN Client macOS improvements in version 2.01 Rel Build 0047

New features

- The LANCOM Advanced VPN Client shows usage examples and configuration hints. By clicking the information additional details will be displayed in a browser.
- The LANCOM Advanced VPN Client can be minimized permanently.
- EAP support (Extensible Authentication Protocol) for 802.1x authentication in a LAN
- Each VPN profile can be configured to either use the providers DNS server or the one accessible through the VPN tunnel.
- Automatic WEB proxy server recognition without password authentication during online activation when using OS X

Bugfixes / improvements

- Solved problems when importing profiles

Advanced VPN Client macOS improvements in version 1.01 Rel Build 0010

Bugfixes / improvements

- The firewall of the LANCOM Advanced VPN client remains active even after a long-lasting system boot (e.g. due to deleting the system cache).
- An internet connection established by OS X via PPPoE (e.g. UMTS) can be used for VPN connection establishment.
- LANCOM Advanced VPN Client can only be started once at a time on the same computer. This avoids overwriting settings of the first user on quick user changes. The VPN connection remains established.
- Fixed the IP address assignment when importing profiles.
- If the LANCOM Advanced VPN Client is used behind a NAT device, the IKE keepalive packets do not avoid link disconnection by manually configured timeouts.
- The firewall log is continued, even if a network adapter is removed or a PPP connection is terminated.
- Reworked error messages in the log window
- A certificate connection which was initialized after application start can be established even if the preset profile was not changed before.